Aritmética modular

Problemas de Criptología - Hoja 2

Curso 07-08

1 **La función parte entera**. Prueba las siguientes propiedades de las funciones parte entera y techo.

(a) $\lfloor x \rfloor \leq x \leq \lceil x \rceil$.

(b) $\lfloor x \rfloor = -\lceil -x \rceil$.

(c) Si k es un número entero, entonces $\lfloor \frac{k}{2} \rfloor + \lceil \frac{k}{2} \rceil = k$.

(d) Si $x \in \mathbb{R}$ y $x \in \mathbb{Z}$, entonces se cumple que $\lfloor x + k \rfloor = \lfloor x \rfloor + k$.

2 **Algoritmo de Euclides**. Calcula, usando el algoritmo de Euclides, el máximo común de las parejas $(21, 9)$, $(105, 15)$, $(119, 95)$ y $(12.240, 13.320)$. Lleva la cuenta de los números r_k, q_k, x_k e y_k. Calcula los coeficientes de Bezout para cada pareja también.

3 **Máximo común divisor.** ¿Cómo se calcularía el máximo común de tres enteros positivos a, b, c? ¿Se puede usar el algoritmo de Euclides? Generalízalo al cálculo del máximo común divisor de k números enteros.

4 **Ecuaciones** $ax+by = n$. Determina cuál de las siguientes ecuaciones tienen solución y cuando sea así, calcularlas.

(a) $1.180x + 482y = 16$.

(b) $12.345x + 1.111y = 17$.

(c) $323x + 306y = 15$.

(d) $210x + 273y + 231z = 42$.

5 **Inversos multiplicativos en** $\mathbb{Z}_n$. Halla los inversos multiplicativos de las siguientes clases, cuando existan:

(a) 7 en $\mathbb{Z}_{23}$.

(b) 8 en $\mathbb{Z}_{27}$.

(c) 6 en $\mathbb{Z}_{81}$.

6 **Grupos**. Consideremos $\mathbb{Z}_n$ y dentro de él todas las clases k tales que $(k, n) = 1$. ¿Forma este conjunto un grupo con la operación de multiplicar?

7 **Matrices**. Efectúa las siguientes operaciones con matrices:

(a) En $\mathbb{Z}_6$:

$$\begin{pmatrix} 1 & -2 & 4 \\ -1 & 5 & 6 \end{pmatrix} + \begin{pmatrix} 5 & -5 & 4 \\ -3 & 0 & 3 \end{pmatrix}, \begin{pmatrix} 5 & -4 \\ 3 & -2 \end{pmatrix} \cdot \begin{pmatrix} -4 & 2 \\ 5 & 3 \end{pmatrix},$$

$$\begin{pmatrix} 3 & 0 \\ -4 & -2 \end{pmatrix} \cdot \begin{pmatrix} 5 & -5 \\ -4 & 2 \end{pmatrix}.$$

(b) En $\mathbb{Z}_7$ calcula los determinantes y las inversas de :

$$A = \begin{pmatrix} 6 & 4 \\ 2 & 5 \end{pmatrix}, B = \begin{pmatrix} 1 & 3 & 4 \\ 2 & 5 & 6 \\ 3 & 6 & 2 \end{pmatrix}.$$

8 **Congruencias de matrices**. Determina cuáles de las siguientes parejas de matrices son congruentes en $\mathbb{Z}_8$:

$$\begin{pmatrix} 12 & -4 \\ 14 & 77 \end{pmatrix} \text{ y } \begin{pmatrix} 44 & 100 \\ 22 & -11 \end{pmatrix}, \begin{pmatrix} -79 & -4 \\ 96 & 108 \end{pmatrix} \text{ y } \begin{pmatrix} 101 & 104 \\ 46 & 94 \end{pmatrix}.$$

9 **Aplicaciones lineales sobre anillos de matrices**. Se considera en $\mathbb{Z}_{11}$ la aplicación lineal dada por la matriz A:

$$A = \begin{pmatrix} -4 & 5 & -6 \\ 2 & 7 & -10 \\ -1 & 3 & 8 \end{pmatrix}.$$

(a) Hallar las imágenes de $(3, 7, 9)$ y $(-5, 9, -10)$.

(b) Hallar el núcleo de la aplicación lineal.

(c) Hallar la aplicación inversa A^{-1} y la imagen de $(1, -1, 3)$ por A^{-1}.